SN Computer Science (2021) 2:77
https://doi.org/10.1007/s42979-021-00471-5

ORIGINAL RESEARCH

Design and Development of a Cyber Security Framework for National Time Dissemination

Amutha Arunachalam[1] · K. Seetharaman[2] · Ashish Agarwal[1]

Received: 5 December 2020 / Accepted: 15 January 2021 / Published online: 6 February 2021

Abstract

Coordinated Universal Time (UTC) is based on the biggest possible number of atomic clocks of various categories, to be found in various regions of the world and connected through a network which allows precise time comparisons amid remote sites. In India, UTC system is followed and cyber security issues are a concern. This research explains the security problems faced with UTC (k) system and describes how enhancement rectifies such problem. There is necessity for single time scale for whole nation. This research adopted qualitative approach and experimental design for carrying out investigation. Data are collected from National Physical Laboratory and National measurement institute of India. Proposed Software to be used in this particular research for implementing the framework is archimate open source. The aim of intention of this research is to design and develop cyber physical security framework for national time dissemination. Security problems are rectified with developed cyber physical security framework. The developed cyber security framework achieves traceability and synchronization in cyber security environment. This research would be helpful for practitioners, academicians, policy-makers, capitalists to understand the need for developing a framework for national time dissemination in cyber-secure environment.

Keywords Cyber physical security · Traceability · Synchronization and national time dissemination · Universal Coordinated Time

Introduction

At first, the concept of Coordinated Universal Time, (UTC), was formulated during 1960s as a means of enhancing the distribution of Universal Time, and to provide the balanced rate of atomic standards in a time signal. The UTC concept has been in practice for more than three decades, and appeared as a rational. Though, the necessities for time keeping have emerged from the classification of UTC. The requirement of a standardized time scale, without the interruption established by the leap seconds, a one-second adjustment, is increasing. UTC makes available the base of civil time, which is related with the legal time of the majority countries. Arias and Guinot [1] stated that local realizations of UTC in time laboratories across the world ensure the diffusion of a time scale which denotes UTC at the intensity of some tens of nanoseconds.

Time zone in India is calculated by GMT/UTC (Greenwich mean time/Coordinated universal time) + 5.5 h. It is also known as IST (Indian Standard Time). Time zone in India is measured based on 82.5° E of longitude at Shankargarh Fort in Mirzapur that is considered as Indian central meridian. Time for daylight saving does not function in India. India is huge nation. It stretches at widest point for 2933 km from east of Arunachal Pradesh to west of Gujarat and covers approximately longitude of 30°. Based on convention, every time zone in globe is spaced by longitude of 15°. Thus, two time zones are there for India. Therefore, government decides to have single time zone around the

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" edited by Rajiv Misra, RK Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ Amutha Arunachalam
amutha@csir.res.in

K. Seetharaman
kseethadde@yahoo.com

Ashish Agarwal
ashish.npl@nic.in

[1] Time and Frequency Metrology, National Physical Laboratory, New Delhi, India

[2] Department of Computer and Information Sciences, Annamalai University, Chidambaram, India

entire nation like China, in spite of different proposals and requests to modify it. This indicates that rises and sets of sun approximately two hours soon on Eastern border of India than in west side of Rann of Kutch [2].

The people, policymakers and capitalists from northeast part of India have been insisting for a separate time zone for a long period of time since they really go through problems with the current IST. The current IST method is considered as a factor that negatively influencing their lives since the sun rises and sets at an earlier time than the so-called official working period. Early sunrise results in loss of daylight hours by the time workplace or academic organizations open. During winter, this issue gets even worse as they witness sunset much early. BIPM has a convenient time scale, referred to as International Atomic Time (TAI), for a consistent sequential reference of time. TAI is a standardized and very balanced scale, however does not keep in pace with the asymmetrical rotation of the Earth. Consequently [3], for public and convenient uses, UTC comes to practice, which is similar with TAI, apart from time to time a leap seconds are included to make sure that, while averaged over a year, the sun traverses through the Greenwich meridian at midday UTC to within 0.9 s.

Globally, many laws, policies and systems, public expectations and technologies necessitate that communal timekeeping stick to Universal Time. The use of two similar systems, UTC and Stepped Atomic Time (SAT), was considered as a stage in the evolution and implementation of a single, convenient and globally acceptable system. The resultant UTC time-scale relay globally, with its potential "jumps" in time, started to cause interests amongst users that looked for stable time scales. There was a growing demand for accurate frequencies for practical uses. Ahuja [4] pointed out that UTC was suggested as the base of standard time in almost all nations, the time in common practice as dispersed by radio signals.

The more conventional function of primary frequency standards (PFS) intensifies the accuracy level of UTC and sets off a new practical advancement for time-scale algorithms. The growth of time and frequency metrology functions in the various metrology zones strengthens the measures of the BIPM time department to enhance the accuracy of UTC, wherein the management with the Regional Metrology Organizations (RMOs) has an important role. The algorithm for the estimation of UTC has been developed to assure the reliability, long-standing frequency stability, increased frequency accuracy level and ease of access of the time-scale. It depends on clock readings and is increasingly reliant on the superiority of the clock comparisons. Panfilo and Arias [5] specified that the BIPM, in a corresponding strength with the world timing society, is devoted to developing and enhancing these techniques.

Lokhorst [6] mentioned that same moment in time could be represented in numerous ways. Every representation could store one or more different information pieces. If the information is more, then extensively adopt Date Time unit. For instance, time is represented in unique way in opening ceremony during start of winter Olympics in 2014 in Sochi, Russia and it is illustrated in Table 1.

Above representations deal with same moment in time and at the same time, they are different in quantity of information given. A local time and date along with UTC offset could be changed to UTC time and date but not vice versa Tables 2, 3, 4.

Synchronization of time is distributing reference of time to real-time clocks in the network of telecommunication. All linked nodes have right to acquire information about time or during every reference period in timing signal is noted and dated as well as distribute a timescale commonly and associated epoch (inside the related requirement for time accuracy). Timescales examples are TAI, UTC, GPS, PTP, UTC + offset (for example local time) and local arbitrary time. Distributing synchronization of time is one way to achieve synchronization phase [7].

Due to unfixed modes in communication and multifaceted interconnection between physical components and layer of cyber information, channels for communication are at risk to malicious attacks which would increase security problems in cyber public system. There are different attacks in CPS like availability attacks [8–10], integrity attacks, such as replay attack [11], deception attack on the basis on innovation [12] false-data injection [13, 14]. GPS (global positioning system) signal is extremely free, stable and accurate for timing, measuring devices based on GPS are implemented in main infrastructures for guaranteeing the synchronization of time between subsystems and therefore reach desirable performance. At the same time, malicious agents would affect the synchronization of time among sensors by implementing counterfeit signals of GPS [15]. Few prior researchers [16–19] and

Table 1 Time and date and its information

Time and date	Information about time
2014-02-07T16:14:00Z	Information with single piece, helpful for server logs in which locations are not appropriate
2014-02-07T20:14:00+04:00	Information with two pieces, helpful for times of package delivery or vacation photo
2014-02-07T20:14:00+04:00 Europe/Moscow	Information with three pieces, required when changing date times or to store future dates

Table 2 Time synchronization

S. no	Author and Year	Purpose of research	Findings
1	Agarwal et al. [22]	Time distribution techniques	The purpose of advancement is to meet the national requirements of e-governance, digital archiving, cyber security, enhanced communication systems, internet of things, etc
2	Marangos et al. [23]	Time synchronization	Physical localities can be in different geographical regions and accordingly distinctive time zones but as well virtualized services might be familiarized to the time zones of their web patrons
3	Khediri et al [24]	Application of Time synchronization	Any variation of time, several application of time synchronization procedure could become non-repudiable employing public key cryptographic systems
4	Schneider [25]	Time synchronization	Time synchronization allows to harmonize the internal clocks of every complex PowerLogic™ ION™ devices

Table 3 Security issues in time synchronization

S. no	Author and Year	Purpose of research	Findings
1	Yang et al. [29]	Security vulnerabilities in time synchronization	In the external attack, a third party could eavesdrop on or change messages but could not find the secret key. Consequently, it is not able to copy a legitimate node; whereas an internal attacker could obtain legal characteristics since it identifies the secret key
2	Zhang et al. [16, 19]	Impact of time synchronization	TSA is developed to deal with the timing information
3	Lisova [8, 28]	Threat and vulnerability analysis	Safety and security interface is as well considered to observe which implications the developed security system has on the safety realm
4	Yadav and Yadav [30]	Synchronization attack	Secured SMMTS protocol is developed to find and disprove message manipulation attacks
5	Guo et al. [27]	time synchronization attack	Effective algorithm was developed to compute the optimal attack, which takes-off the least amount of sensors and results in uncontrolled average estimation fault covariance
6	Barreto [26]	Cyber-attack on packet-based time synchronization protocols	It could be effectively performed irrespective of the cryptographic behavior that the PBTSP is defended with

Table 4 Existing studies

S. no	Author and Year	Purpose of research	Findings
1	Levesque and Tipper [34]	PTP standard	For highly precise performance in synchronization, support of hardware is needed for precise timestamping and residence times
2	Kyriakakis et al. [35]	Engineering issues in communication of time-triggered (TT) and distribution scheduling of task over Ethernet switch	Messages of TT were switched from server node to client that control duty cycle of two signals of pulse width modulation
3	Paul et al. [37]	CPS test	Combined the proposed CPS test into network of time-sensitive networking
4	Suzuki et al. [33], Kadowaki and Ishii [32], Kikuya et al. [31]	Time synchronization	Studied about synchronization problems

real-world attacks in GPS spoofing have indicated the GPS signals' vulnerability and probability of spoofing the receivers in GPS [20]. According to Wang [21], any successful synchronization of time attack that inserts virtual offsets on sensor clocks and at the same time target system is desynchronized would result in huge degradation in performance.

Objectives of the research are as follows:

(i) To investigate the need for developing framework for national time dissemination
(ii) To study about security issues faced with UTC (k)
(iii) To develop and design a cyber physical secure framework for national time dissemination
(iv) To examine about performance of cyber physical secure framework in cyber-secure environment.

There are numerous studies that focused on time synchronization, such as Agarwal et al. [22], Marangos et al. [23], Khediri et al. [24], Schneider [25]. Authors also focused on security issues in time synchronization [8, 16, 19, 26–30]. Fault-tolerant synchronization of clock studied by Kikuya et al. [31], event-based distributed synchronization of clock was investigated by [32]. Simulations of CPS like CPS co-simulator framework were studied by [33]. However, there are no specific studies focused on designing and developing cyber physical secure framework for national time dissemination. Therefore, this particular research intends to focus designing and developing cyber physical secure framework for national time dissemination. Performance of developed framework achieves traceability and synchronization.

Literature Review

Time Synchronization: An Overview

According to Agarwal et al. [22], the protector or developer of primary time-scale generating IST is CSIR-National Physical Laboratory (CSIR-NPL), New Delhi. The current paper reports the primary reduction of the improbability of Primary Time-Scale from 20 to 7.2 ns and ultimately to 2.8 ns. The paper also discusses present time distribution techniques being used and the activities undertaken for advancement and amplification of the primary time-scale to contribute to the country in a better way at the same level with the global level. The purpose of advancement is to meet the national requirements of e-governance, digital archiving, cyber security, enhanced communication systems, internet of things, etc. To conclude, this article explained the tasks undertaken to improve the primary time-scale and its distribution capabilities to users like Indian Space Research Organization (ISRO).

As any typical forensic investigation gives rise to the law court, the study has also dealt with the existing position of the related legislation, bearing in mind that the study intends to examine technical audience. The time synchronization is of major significance as well for the investigation logs to be employed as basis of evidence. A necessity that clearly is not simple to accomplish, particularly in a cloud context wherein the cloud server and the client are generally to be found in various time zones: not only physical localities can be in different geographical regions and accordingly distinctive time zones but as well virtualized services might be familiarized to the time zones of their web patrons [23].

Khediri et al [24] expressed that synchronization is essential aspect of successful and effective operations in every business settings as they depend on the data accuracy level to make fast and effective decisions. In general, the proposed techniques necessitate that all sensor nodes have a collective time scale in order that the central unit could synchronize and coordinate between sensors to achieve their tasks. Yet, it is complicated to maintain a common time-scale for all sensors. Acceptability of evidence could be forced with technological proofs. These days, contemporary cryptography provides the tools for incontestable clock management. Any variation of time, several application of time synchronization procedure could become non-repudiation employing public key cryptographic systems. Though, these techniques are not supported by the current time synchronization applications.

As reported by the report of Schneider [25], time synchronization signals are transmitted at regular intervals periodically over the network, every meter constantly evaluates its capability to remain coordinated with the external broadcasts. Time synchronization allows to harmonize the internal clocks of every complex PowerLogic™ ION™ devices. Once harmonized, every data log has time stamps which are corresponding to a standardized time base, which empowers to accomplish accurate series of events and power quality assessment.

Security Issues in Time Synchronization

Yang et al. [29] studied about security vulnerabilities in time synchronization, with regard to Time-slotted channel hopping (TSCH). Time synchronization is extremely essential for the TSCH-based wireless networks. Though, the time-synchronization behavior in TSCH networks focuses on only clock accuracy whilst paying no attention to security issues. If an opposition initiates time-synchronization damage on a network, the whole network communication system would possibly be paralyzed. There are various secure time-synchronization etiquettes in WSNs (for example SPS and SMTS). In the current study, time synchronization in networks is classified into single-hop, cluster-wise, and multi-hop in line with the network scope. The study analyzes their security attacks, because of the high-precision synchronization conditions and finds out some particular attacks and later presents related security countermeasures. The study dealt with Dolev-Yao threat model, which is a standard attack model wherein the attacker could eavesdrop, change, or falsifies communication messages in the system. The two kinds of attack considered in the study are external and internal. In the external attack, a third party could eavesdrop on or change messages but could not find the secret key. Consequently, it is not able to copy a legitimate node, whereas an internal attacker could obtain legal characteristics since it identifies the secret key.

Zhang et al. [16, 19] studied the impact of time synchronization. Fault detection and event location assessment are generally based on accurate timing information. In the current study, a new Time Synchronization Attack (TSA) is developed to deal with the timing information. As many applications use synchronous measurements and the majority of the measurement appliances are provided with global positioning system (GPS) for accurate timing, it is increasingly likely to harm the measurement system by bluffing the GPS. The efficiency of TSA is established for three applications of device known as phasor measurement unit (PMU) in smart grid, i.e. communication line fault identification, voltage stability monitoring and event location. The strength of TSA is exhibited by arithmetical simulations.

As stated by Lisova [8, 28] in current society, increasingly more embedded systems are connecting. There are various kinds of embedded systems, such as industrial networks, connected vehicles, etc. Generally, such cyber physical systems (CPS), irrespective of their information, have a communication part which empowers data exchange amid system and external entities. In this paper, a threat and vulnerability analysis of time synchronization is created upon IEEE 1588, a standard extensively employed in sector for instituting and maintaining clock synchronization. Safety and security interface is as well considered to observe which implications the developed security system has on the safety realm. After all, the monitoring technique is summarized and assessed for various estimations of channel consistency to examine the pertinence of the solution in various settings, and consequently a method for black-channel state manager model is given.

Yadav and Yadav [30] specified that time synchronization is a fundamental specification for different applications. In every synchronization attack, the objective is to influence nodes in some way that their adjacent nodes are at a several time then they actually are. As global synchronization is the aim for certain protocols and they depend on the adjacent nodes to transmit the synchronization data on, negotiating a node would interrupt the international synchronization. The lately proposed maximum and minimum time synchronization protocol (MMTS) is a potential alternate model since it does not base on some network topology. However, MMTS is exposed to various message manipulation attacks. The study focuses on how to protect the MMTS protocol in WSNs under message exploitation attacks. In addition, the study investigates the effect of message exploitation attacks over MMTS. Followed by, a novel Secured SMMTS protocol is developed to find and disprove message manipulation attacks.

Study by Guo et al. [27] take time synchronization attack into account against multi-system scheduling wherein numerous sensors examine various linear dynamical methods and plan their transmissions through a communal rear-ender channel. The study exhibits that by arbitrarily inserting relative time balances on the sensors, the spiteful attacker is capable of making the anticipated estimation error covariance of the entire system differs without certain system knowledge. For the circumstances that the third party has complete system information, the study proposes an effective algorithm to compute the optimal attack, which takes off the least amount of sensors and results in uncontrolled average estimation fault covariance. To moderate the attack outcome, the study further proposes a counteraction by developing shift invariant communication policies and classifies the lower and upper boundaries for system assessment performance. To conclude, simulation examples are presented to demonstrate the acquired results.

Barreto [26] presents a study about cyber-attack on packet-based time synchronization protocols (PBTSP) with increased-accuracy specifications. The cyber-attack is untraceable from the PBTSP's views and manipulates a vulnerability which is in the nature of every PBTSP. It could be effectively performed irrespective of the cryptographic behavior that the PBTSP is defended with and it is untraceable by the algorithm known as clock-servo within the target slave clock. To execute this cyber-attack, the study builds a "Delay Box" able to advance or delay a slave clock by establishing a spiteful offset of a few microseconds. The paper runs experimental analysis to the delay box to demonstrate the extent of the attack and to authorize imperceptibility. In conclusion, the study discusses potential countermeasures for this kind of attack.

Existing Studies

For all protocols based on packet synchronization, main problem is to avoid end-to-end delays in asymmetric. Such delays happen because of processing delays, transmission and queuing. For solve this main issue, transparent clocks were initiated in PTP standard that estimates the queuing delays, processing and routing for correcting asymmetric delays. Further classified into configuration, hardware- and software-based techniques, configuration and software-based approaches with the help of PTP standard at reasonable cost as no new equipment of hardware is needed and could give performance in microsecond synchronization. At the same time for highly precise performance in synchronization, support of hardware is needed for precise timestamping and residence times. In addition to that, security is main challenge to safeguard the timing messages against illegal attackers disrupt services as well as leads to failure and damage to equipment [34].

Kyriakakis et al. [35] studied engineering issues in communication of time-triggered (TT) and distribution scheduling of task over Ethernet switch. Synthetic application of CPS is deployed and estimated the experimental set-up design that involves three nodes: 2 actuation nodes which control 2 servo motors and 1 time server. Messages of TT were switched from server node to client that control duty cycle of two signals of pulse width modulation. Even though authors evaluated and explained experimental scheme of TT communication and collect 1st outcomes on negative impacts of non-cooperative traffic in the flows of TT, more investigation is required to measure the miss rate at client node and achieving synchronization of time [36], quality relying on the injected traffic in the network. At the same time, authors planned to combine the proposed CPS test into network of time-sensitive networking and was done based on research [37]. Authors repeated the experiment within a time-triggered Ethernet network and wound up with set of hardware and software components for node of end-system required to attain time-triggered communication in real-time networks in Ethernet.

Authors also presented a framework to perform exact numerical simulations of CPS, namely CPS co-simulator [33]. Researchers also studied about event-based distributed synchronization of clock for fixed sensor networks [32]. Kikuya et al. [31] focused on fault-tolerant synchronization of clock over unreliable channels in networks of fixed sensor.

Technical Gaps

Information assets, such as data and information systems, should be confined from security threats. There are even some gaps existed and these are considered very representative of current complications and challenges in Cyber Security Framework. In consequence, it is essential to upgrade existing standards and develop a new process, such as cyber risk management, to deal with the various gaps. Security issues and challenges in the UTC system have become a major issue across the world, and accordingly developing secure and efficient CPS is considered extremely essential. In consequence, this study makes an attempt to bridge this gap. The study also stands unique by developing a framework for national time dissemination in cyber-secure environment.

Research Methodology

Main intention of the research is to design and develop cyber security framework for national time dissemination. Qualitative research is kind of investigation in science. It searches answers to research question, gathers evidence and so on. It is efficient in getting culturally particular data about social contexts, behaviours, values and opinions of specific inhabitants [38]. This research adopts qualitative research for designing and developing cyber security framework for national time dissemination. An experimental design of the research is about blueprint of methods engaged in answering the question of the research. It is completed plan to carry out the scientific investigation. Investigators visualize a design of the research for any examination not merely on basis of notion or convenience. There are different criteria and methods for classifying research design, namely experimental and non-experimental design. Experimental design encompasses adopt of some form of intervention or experiment [39]. This research makes use of experimental design for carrying out the investigation. For experimental research, data are collected from National Physical Laboratory and National measurement institute of India. Software used in this particular research for implementing the framework is archimate open source Fig. 1.

Proposed System

Figure 2 illustrates CPS framework: identity, analyze and address. Identify framework of CPS, these are the regions of utilization of CPS wherein stakeholders might have cross-domain concerns. Identify cross-cutting concerns are another important aspect, such as social, business and technological, etc. Shareholders could have concerns which intersect or are examples of wider conceptual concerns. It also addresses concerns by means of various activities and artifacts systematized within three basic components of conceptualization, realization, and assurance. Aspects of CPS are functional, lifecycle, data, business, composition, human, timing, boundaries and trustworthiness. Facets of CPS are realization, assurance and conceptualization. CPS

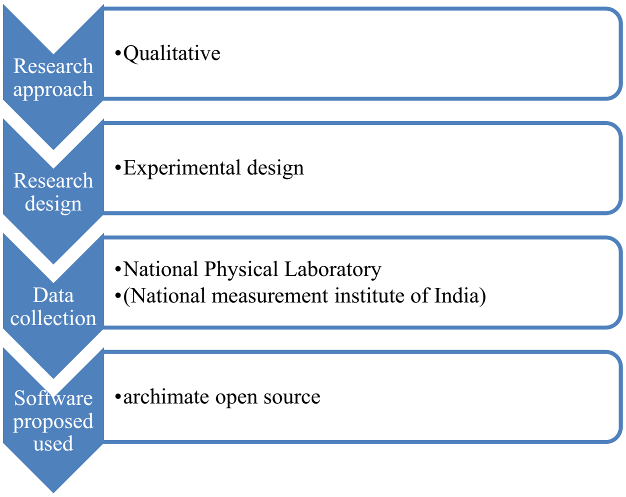

Fig. 1 Overall representation of research methodology

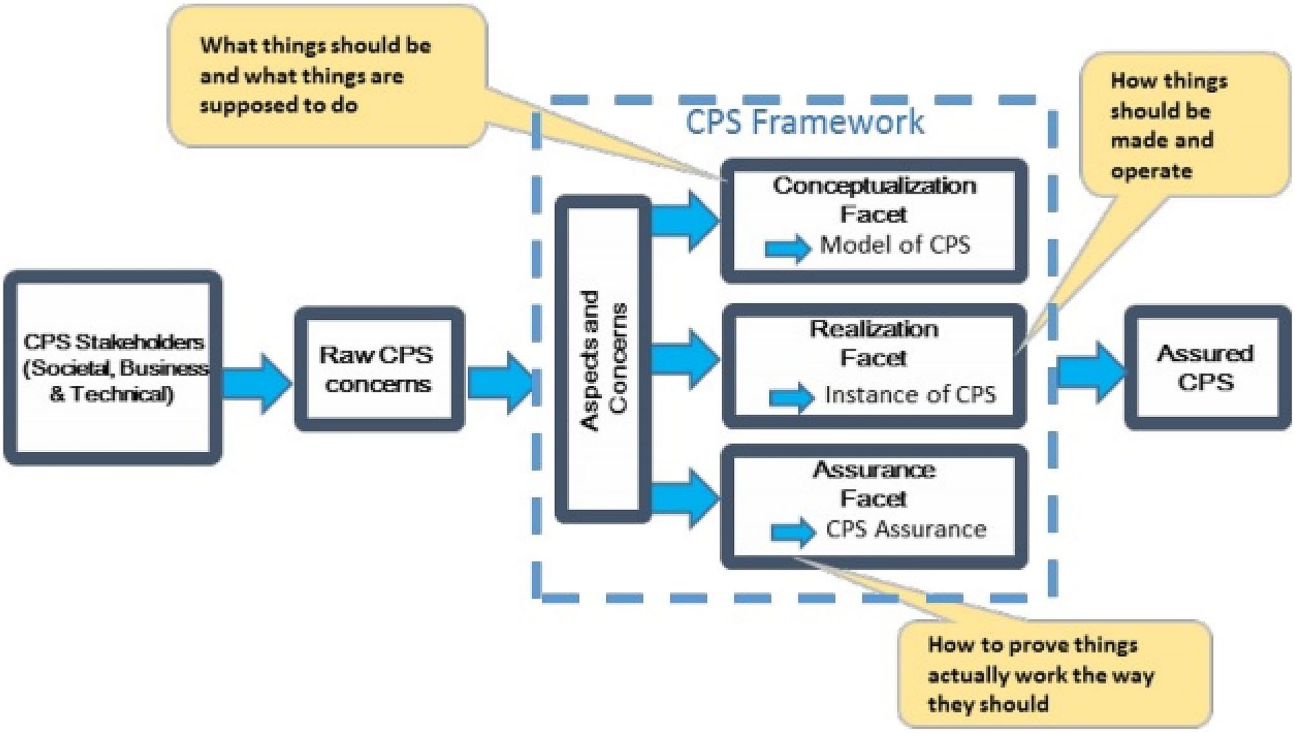
What things should be and what things are supposed to do
CPS Framework
How things should be made and operate
CPS Stakeholders (Societal, Business & Technical)
Raw CPS concerns
Aspects and Concerns
Conceptualization Facet
Model of CPS
Realization Facet
Instance of CPS
Assurance Facet
CPS Assurance
Assured CPS
How to prove things actually work the way they should

Fig. 2 Overview and derivation of CPS framework

includes components, such as digital, analog and human, originated for functions through unified physics and logic. CPS and associated systems are broadly identified as having increased potential to facilitate inventive applications and influence various economic sectors in the global economy. These application domains include infrastructures, building control, healthcare, etc. The CPS Framework in any domain presents an organized management of a CPS method on the basis of its core concepts of domains, facets and aspects [40]. CPS as well includes conventional operational technology (OT) in order for controlling aspects and catalyst. As stated by Griffor et al. [41, 42], the combination of information and traditional technology worlds along with related timing limitations is a specifically new feature of CPS. A CPS function can be a System of Systems (SoS) [43]. Per se, it might link manifold purposes, and also time and data domains, therefore necessitating methods of translation amongst these domains. For instance, different time domains might refer different timescales or have typical accuracies.

Figure 3 represents time scale system UTC 9k)–CSIR NPL time scale system (IST). In the domain of time and frequency altitude, the preferred reference is generally UTC, or one or more than that of its authorized realizations, known as UTC (k), and traceability to UTC is an authorized condition for many entities. Traceability to UTC could be formulated in three areas including frequency, time interval, and time-of-day synchronization. Time signals, integrating those diffused by GPS satellites and system time servers, could be used to institute legal metrological traceability to UTC all through a UTC (k) timescale. These signs have small adequate uncertainties to address industrial synchronization and traceability necessities, but users are accountable for having adequate evidence to show that their necessities are being addressed. Matsakis et al. [44] pointed out that an important part of this signal is the capability to exhibit that an uninterrupted sequence of calibrations back to UTC through a UTC (k) laboratory subsists, and that every linkage of the traceability chain has a standard measurement uncertainty.

Figure 4 illustrates about timescale management system. It explains about timescale system UTC (k) system cybersecure physical framework for UTC–NPLI. Timescale management system is categorized into subsystem. Clock ensemble comes under subsystem 1. Measurement system comes under subsystem 2. Satellite receivers come under subsystem 3. Facility management system comes under subsystem 4. Central processing system comes under subsystem 5. Component Monitor and Control System comes under subsystem 6. Timescale distribution system comes under subsystem 7.

Clock Ensemble (General): Subsytem1

A local recognition of UTC (k) is seen as main reference in the system of national time dissemination. Design of UTC (k) adopts a collection of 3 active hydrogen masters

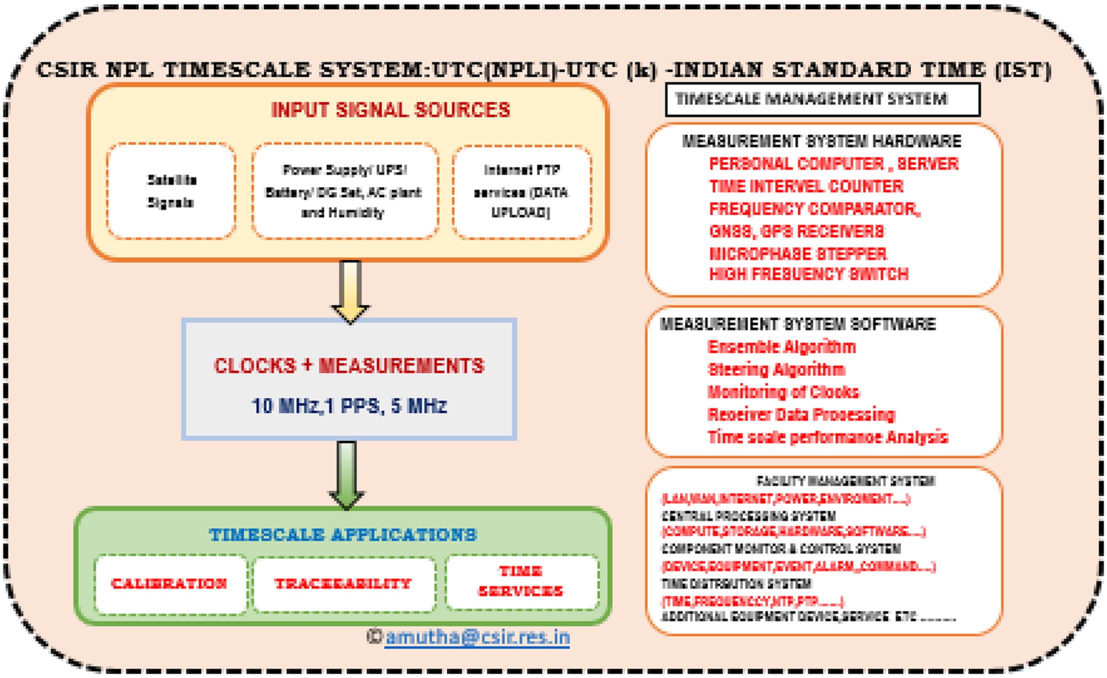
CSIR NPL TIMESCALE SYSTEM:UTC(NPLI)-UTC (k) -INDIAN STANDARD TIME (IST)
INPUT SIGNAL SOURCES
Satellite Signals
Power Supply/ UPS/ Battery/ DG Set, AC plant and Humidity
Internet FTP services (DATA UPLOAD)
CLOCKS + MEASUREMENTS
10 MHz,1 PPS, 5 MHz
TIMESCALE APPLICATIONS
CALIBRATION
TRACEABILITY
TIME SERVICES
©amutha@csir.res.in
TIMESCALE MANAGEMENT SYSTEM
MEASUREMENT SYSTEM HARDWARE
PERSONAL COMPUTER , SERVER
TIME INTERVEL COUNTER
FREQUENCY COMPARATOR,
GNSS, GPS RECEIVERS
MICROPHASE STEPPER
HIGH FREQUENCY SWITCH
MEASUREMENT SYSTEM SOFTWARE
Ensemble Algorithm
Steering Algorithm
Monitoring of Clocks
Receiver Data Processing
Time scale performance Analysis
FACILITY MANAGEMENT SYSTEM
(LAN,WAN,INTERNET,POWER,ENVIROMENT....)
CENTRAL PROCESSING SYSTEM
(COMPUTE,STORAGE,HARDWARE,SOFTWARE....)
COMPONENT MONITOR & CONTROL SYSTEM
(DEVICE,EQUIPMENT,EVENT,ALARM,,COMMAND....)
TIME DISTRIBUTION SYSTEM
(TIME,FREQUENCCY,NTP,PTP.......)
ADDITIONAL EQUIPMENT DEVICE,SERVICE ETC ....

Fig. 3 TIME Scale System UTC (k)–CSIR NPL Timescale system (IST)

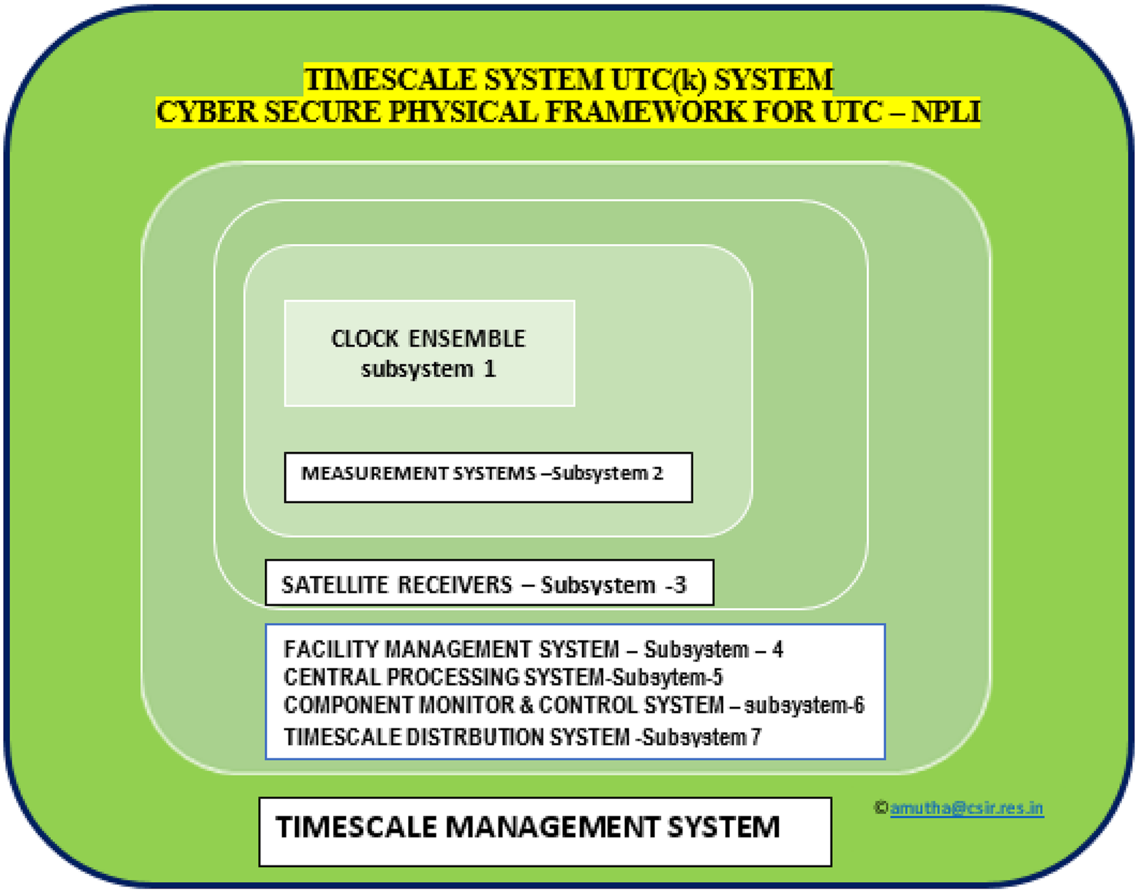
TIMESCALE SYSTEM UTC(k) SYSTEM
CYBER SECURE PHYSICAL FRAMEWORK FOR UTC – NPLI
CLOCK ENSEMBLE subsystem 1
MEASUREMENT SYSTEMS –Subsystem 2
SATELLITE RECEIVERS – Subsystem -3
FACILITY MANAGEMENT SYSTEM – Subsystem – 4
CENTRAL PROCESSING SYSTEM-Subsytem-5
COMPONENT MONITOR & CONTROL SYSTEM – subsystem-6
TIMESCALE DISTRBUTION SYSTEM -Subsystem 7
TIMESCALE MANAGEMENT SYSTEM
©amutha@csir.res.in

Fig. 4 Timescale management system

for offering redundancy and monitoring the performance of maser in real time. Clock ensemble encompasses PMS (phase micro-steppers) for guiding the phase and timescale frequency without distributing masers themselves. PMS are chosen for low added noise in phase without affecting ensemble performance. Once ensemble of time is fully calibrated and operational, only frequency guides to PMS to track UTC closely. For every few years, hydrogen masers must be re-tuned or else they would move too away from the output frequency in the design. Timing uncertainty given by clock system must be considerably below the other uncertainty sources, so that it does not influence overall sensitivity of timing in the system of primary timescale.

UTC (NPLI) Clock Ensemble

Presently, in set-up of state-of-the-art timescales, known as primary timescales, are expanded using five caesium clocks, measurement system, one hydrogen maser and links for international satellite for comparison of clock and link of traceability. Caesium clocks give complete atomic time reference that has outstanding long-term stability, while hydrogen maser has final stability in short-term. UTC (NPLI) is recognized as guided output of AHM (active hydrogen maser). Ensemble of timescale has five Caesium clocks with high performance.

Measurement system: Subsystem 2

Using the measurement system and calibration of frequency and time, it is probable for calibrating Rb standards of atomic frequency, Cs atomic clocks, signal generators, counters, standards of quartz frequency, spectrum analyzers, chronometers, tachometers and timers. Measurement capabilities and calibration of the system are needed for uncertainty of frequency measurement, frequency range, measurement of time interval, measurement uncertainty of time interval, uncertainty of amplitude measurement, amplitude range, measurement of modulation parameter, measurement of phase noise. Recognition of international traceability of UTC (k) primary time scale to BIPM encompasses signal analysis capabilities and measurements of phase noise. For ensuring that stamping of time in received signals are traced to local standard of time, a full end-to-end calibration in chain of time distribution is required to every node in system.

Satellite Signals: Subsystem-3

Global navigation satellite system (GNSS) satellites system giving autonomous geo-spatial positioning and recovery of frequency or time with global coverage, permitting receivers to identify their attitude, time, longitude and latitude using signals of time transmitted by radio to receive line-of-sight from satellites. Present GNSS entails the European Union's Galileo, China's Beidou systems, United States' GPS, Russia's GLONASS.

GNSS Receiver: It is adopted for receiving signals from GNSS are compared against the timescale of UTC (k). BIPM could adopt such measurements for computing timescale of UTC (k) time offset. There are different techniques there for processing of data. Most commonly adopted is PPP (Precise point positioning) that is regularly used by BIPM.

Facility Management System: Subsystem 4

Systems in timescale implemented sites encompassing sites in disaster recovery required to be conditioned with precision AC system on basis of 24/7. Absolute rooms' temperature must be kept within 20 ± 2 °C. Room must be conditioned with dual UPS (uninterrupted power supply) on basis of 24/7. Supplies of power must be controlled and made accessible through STS (static transfers witch). Monitoring console is there in the workstation room to monitor and characterize the system of timescale. Earth pits are there for earthing for equipment of timescale and atomic clocks. Needed earth strips are there within the room. Further lighting arrestors on top of the roof are ensured. Internal temperature and fans of the equipment are monitored for detecting failures at initial stage and for informing a proactive strategy for replacement if necessary.

Central Processing System (CPS): Subsystem 5

CPS gives control interfaces in top level and coordinates more loosely coupled services and lower levels workflow. CPS gathers data regarding health service and universal operational status using data is divided between controllers of master that is accountable for maintaining and starting services and controller for processing which handling processing execution and less scheduling. CPS would harmonize difficult performance within system of timescale and other system parts. Main drivers of CPS modules are consistency and accessibility. CPS modules are performed in such a way that functionality in controlling is allocated among processing block controller, processing controller and master controller. Allocated control assures the requirement of reliability and availability are meant by CPS.

Component Monitor and Control System (CMCS): Subsystem6

Tiered approach was deployed in CMCS of UTC (k). Primary timescale involves a many components on the basis of commitment where CMCS would carry out. Every stage in component controls, monitors and manages all other UTC

(k) elements through control and monitor systems, local to every component which in-turn stage-control, monitor and manage respective elements. Apart from these, local system gets commands from such system to control that are interpreted into commands at low level by local systems as well as transmit to component equipment. CMCS components collect monitoring information from each of equipment in component and transmit it up to CMCS.

Timescale distribution system (TDS): Subsystem 7

TDS would give timing information using NTP from system of primary timescale. Networks have suitable and sufficient security against external threats. No failure would be seen in the system of time dissemination. Such system would supply for at least clients/sec for NTP. Such system has to support minimum 20 point to point offered links for serving priority clients. Every system could have minimum two fixed internet IP focused on distributed to assure high availability.

Discussion

India will possibly have two time zones. Though, the Government of India prefers to keep a single time zone across the entire nation, regardless of a number of requests and suggestions to change it. The state Government of Assam aims to introduce the single time zone across the entire state and rest of the other northeast part of Indian states [45]. Ahuja et al. [4] discussed the benefits of advancing IST in terms of energy-saving. However, the Government of India is keen to keep one time zone to inhibit confusion and security issues. National Meteorology Institute (NMI) transmits their clock data to BIPM and latter estimates the actual international time scale (TAI) on the basis of these data. For instance, in the United States, legitimate time is categorized into nine standard time zones together with DST [3].

Cyber-physical systems (CPS) as an advanced system include engineered interrelating networks of physical and computational components. CPS can interrelate with humans by means of several new modalities. It is generally considered as having great prospective to facilitate innovative applications and influence various economic divisions in the global economy. As CPSs interact with their environs, synchronized requirements and relevance are of fundamental nature, since there are time limits to be acquainted with system responses [46]. The proposed CPS framework in the study presents a set of advanced concepts, in which their goal is to present a common language for defining interoperable CPS architectures in different domains. The three facets of CPS include conceptualization, realization, and assurance is presented in detail. Each facet is exhibited and understood from its set of artifacts. As discussed in the paper, security, reliability in addition to safety, against spiteful and also natural attacks and conditions, could be figured out as one of the important challenges in CPS design [47]. With more CPSs interconnecting to the surrounding network, the threat to impairment that caused deliberately is greater than ever. Consequently, as stated by Schneider [48], there is a demand to synchronize safety and reliability engineering such that the difficult risk of harm as a result of either faulty or spiteful intention is sufficiently addressed.

Conclusion

Time is the primary metadata which deal with a log-record. Though, the complicated problem of timekeeping in conventional systems becomes almost a burden for logging system designers, and regrettably, the problem of time synchronization and traceability has been underrated from the research community. The study particularly carried out to design and develops a novel system for cyber security framework in the context of national time dissemination. CPS is extensively identified as having great potential to authorize inventive applications and influence multiple sectors in the global economy. The developed framework in the study will be revolutionary and invasive. Examining the challenges and prospects of CPS involves broad accord in foundational conceptions, and a collective understanding of the critical new potentials and technological systems unique to CPS. A knowledge gap still subsists with regard to establishing the science of cyber security for UTC. In this context, in other technological fields, a systematic technique is typically proposed and applied to deal with these demands. The advantage of such a science is the growth and analysis of theories which result in comprehending the wide removal of cyber threats and the capability to analyze trade-offs in supporting network missions whilst reducing attacks.

The advancement of UTC has adhered to the scientific and industrial growth by formulating appropriate paradigms, more modified calculation algorithms, more effective and fast distribution processes and a well-defined traceability chain. Main aim of the study is to make primary time scale system as CPS framework. Currently, UTC (k) system is followed in India and the Timescale System controlled and monitored as individual subsystems. The availability and fault management of subsystems contributes to the overall robustness and dependability of Timescale system that has significant amount of subsystems that are bound to have malfunctioning of equipment, hardware, software and also exposed to its cyber and Physical risks. Thus, it is significant to have Primary Timescale System UTC(k) in CPS and then enhanced integrated management of PTS should lean to CPS and Time Dissemination used as primary source for national time, then it would achieve resilient and stabilized traceability and synchronization including cybersecurity, privacy, trust including block-chain, distributed archives digital characteristics, trusted and adaptive security architecture, co-engineered safety and security, Such upgraded system is referred as consolidated PTS. For achieving traceability and synchronization, this research had developed framework for national time dissemination in a cyber-secure environment.

Future Scope

The study carried out in a way to address the larger question of retaining mission functionality of a system in cyber-attacks. The study comes to the conclusion that CPS application systems should be designed and developed by considering the progressive technologies, essential system-level requirements, and inclusive effect on the real world. The study has provided an outline of some of the more significant challenges and techniques linked with timing issues in developing and designing CPS framework. Additional studies on design setting which facilitates better specification and authentication of timing requirements are required and also more work in dealing with security issues in time synchronization.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Arias EF, Guinot B. Coordinated Universal Time UTC: historical background and perspectives. 2005. https://pdfs.semanticscholar.org/5051/a2f8fc9144f012a909195d52ed15d892f414.pdf. Retrieved 16 Apr 2020.
2. Cook S (2019) What is the Time Zone in India? https://www.tripsavvy.com/what-is-the-india-time-zone-1539421. Retrieved 18 Aug 2020
3. Sharma L, Kandpal SDP, Olaniya MP, Yadav S, Bhardwaj T, Thorat P, Panja S, Arora P, Sharma N, Agarwal A, Senguttuvan TD, Ojha VN, Aswal DK. Necessity of 'two time zones: IST-I (UTC + 5: 30 h) and IST-II (UTC + 6: 30 h)' in India and its implementation. Curr Sci. 2018;115(7):1252–61.
4. Ahuja DR, Gupta DP, Agrawal VK. Energy savings from advancing the indian standard time by half an hour. Curr Sci. 2007;93(3):00113891.
5. Panfilo G, Arias F. The Coordinated Universal Time (UTC). Metrologia. 2019;56:1–27.
6. Lokhorst T. Why "Always use UTC" is bad advice. 2019. https://engineering.q42.nl/why-always-use-utc-is-bad-advice/. Retrieved 18 Aug 2020.
7. Mizrahi T. Time synchronization security using IPsec and MACsec 2011. In: International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS) 12–16 September; 2011, pp. 38–43.
8. Lisova E. Monitoring for securing clock synchronization. Mälardalen Univ Press Diss. 2018;256:1–186.
9. Qin J, Li M, Shi L, Yu X. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. IEEE Trans Autom Control. 2017. https://doi.org/10.1109/TAC.2017.2756259.
10. Li Y, Shi L, Cheng P, Chen J, Quevedo DE. Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach. IEEE Trans Autom Control. 2015;60(10):2831–6.
11. Mo Y, Sinopoli B. Secure control against replay attacks. In: 47th Annual Allerton Conference on Communication, Control, and Computing; 2009, pp. 911–8.
12. Guo Z, Shi D, Johansson KH, Shi L. Optimal linear cyberattack on remote state estimation. IEEE Trans Control of Netw Syst. 2017;4(1):4–13.
13. Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Trans Inform Syst Secur. 2011;14(1):13.
14. Mo Y, Sinopoli B. False data injection attacks in control systems. In: First Workshop on Secure Control Systems, CPS Week, 2010.
15. Wu S, Ren X, Dey S, Shi L. Optimal scheduling of multiple sensors with packet length constraint. IFAC-Papers Online. 2017;50(1):14430–5.
16. Zhang Z, Gong S, Dimitrovski DA, Husheng L. Time synchronization attack in smart grid: impact and analysis. IEEE Publ. 2013. https://doi.org/10.1109/TSG.2012.2227342.
17. Wang K, Chen S, Pan A. Time and position spoofing with open source projects. London: Black Hat Europe; 2015.
18. Tippenhauer NO, Popper C, Rasmussen KB, Capkun S. On the ¨ requirements for successful GPS spoofing attacks. In: Proceedings of the 18th ACM conference on Computer and communications security; 2011, pp. 75–86.
19. Zhang Z, Gong S, Dimitrovski AD, Li H. Time synchronization attack in smart grid: Impact and analysis. IEEE Trans Smart Grid. 2013;4(1):87–98.
20. Khalajmehrabadi A, Gatsis N, Akopian D, Taha AF. Real-time rejection and mitigation of time synchronization attacks on the global positioning system. IEEE Publ. 2018. https://doi.org/10.1109/TIE.2017.2787581.
21. Wang J, Tu W, Lucas CK, Hui SM, Wang EK. Detecting time synchronization attacks in cyber-physical systems with machine learning techniques. London: IEEE Publications; 2017.
22. Agarwal A, Olaniya MP, Yadav S, Kandpal P, Arora P, Panja S, Das M, Thorat P, Bharadwaj T, Bharath V, Sharma N, Mamta DM, Ojha VN, Aswal DK. Reduction of uncertainty of Primary Time Scale generating UTC(NPLI) to 2.8 ns. URSI AP-RASC 2019, New Delhi, India, 2019.
23. Marangos N, Rizomiliotis P, Mitrou L. Time synchronization: pivotal element in cloud forensics. Secur Commun Netw. 2016;9:571–82.
24. Khediri S, Nasri N, Samet M, Wei A, Kachouri A. Analysis study of time synchronization protocols in wireless sensor networks. 2012. https://arxiv.org/ftp/arxiv/papers/1206/1206.1419.pdf. Retrieved 18 Apr 2020.
25. Schneider Electric Report (2009) Time Synchronization and Timekeeping. https://www.se.com/ar/library/SCHNEIDER_ELECTRIC/SE_LOCAL/APS/208433_2F12/ION_Time_Synchronization_and_Timekeeping.pdf. Retrieved 17 Apr 2020.
26. Barreto S. Cyber-attack on packet-based time synchronization protocols: the undetectable delay box. London: IEEE Publications; 2018.
27. Guo Z, Yuqing N, Wong WS, Ling S (2018) Time synchronization attack and countermeasure for multi-system scheduling in remote estimation. https://arxiv.org/pdf/1903.07036.pdf. Retrieved 17 Apr 2020.

28. Lisova E. Monitoring for Securing Clock Synchronization. Dissertation, Malardalen University, 2018.
29. Yang W, Wan Y, He J, Cao Y. Security vulnerabilities and countermeasures for time synchronization in TSCH networks. Hindawi J. 2018. https://doi.org/10.1155/2018/1954121.
30. Yadav J, Yadav R. Attacks and requirements of time synchronization. Int J Comput Sci Mob Comput. 2014;3(11):598–704.
31. Kikuya Y, Dibaji SM, Ishii H. Fault tolerant clock synchronization over unreliable channels in wireless sensor networks. In: IEEE Transactions of Control of Network Systems, 2018.
32. Kadowaki Y, Ishii H. Event-based distributed clock synchronization for wireless sensor networks. IEEE Trans Autom Control. 2015;60(8):2266–71.
33. Suzuki A Masutomi K, Ono I, Ishii H Onoda T. CPS-Sim: Co-Simulation for Cyber-Physical Systems with accurate time synchronization, IFAC Papers Online; 2018, pp. 70–5.
34. Levesque M, Tipper D. A survey of clock synchronization over packet-switched networks. IEEE Commun Surv Tutor. 2016. https://doi.org/10.1109/COMST.2016.2590438.
35. Kyriakakis E, Spars J, Schoeberl M. Implementing time-triggered communication over a standard ethernet switch. In: Proceedings of the Fog-IoT Workshop 2019. New York: Association for Computing Machinery; 2019.
36. Marina G, Wilfried S, Radu D, Sasikumar P. Synchronization quality of IEEE 802.1 AS in large-scale industrial automation networks. In: Proceedings of the Real-Time and Embedded Technology and Applications Symposium (RTAS). IEEE; 2017, pp. 273–82.
37. Paul P, Michael LR, Silviu SC, Wilfried S. Design optimisation of cyber-physical distributed systems using IEEE time-sensitive networks. IET Cyber-Phys Syst. 2016;1:86–94.
38. Babu RG. Research methodology in social sciences. Delhi: Concept Publishing Company; 2008. p. 11.
39. Blessing LTM, Chakrabarti A. DRM, a design research methodology. Berlin: Springer; 2009. p. 269.
40. Broman D, Derler P, Eidson JC. Temporal issues in cyber-physical systems. J Indian Inst Sci Multidiscip Rev J. 2013;93(31):1–14.
41. Griffor ER, Greer C, Wollman DA, Burns MJ. Framework for Cyber-Physical Systems Overview. NIST Special Publication 1500–201, 2017.
42. Griffor ER, Greer C, Wollman DA, Burns MJ. Framework for Cyber-Physical Systems: Volume 2, Working Group Reports. NIST Special Publication 1500–202, 2017.
43. Hensahw M. Systems of systems, cyber-physical systems, the internet-of-thing. Whatever Next? OR Insight. 2016;19(3):51–4.
44. Matsakis D, Levine J, Lombardi MA. Metrological and legal traceability of time signals. In: Conference: Proceedings of 2018 ION Precise Time and Time Interval Meeting (PTTI), Virginia, 2018.
45. Singh A, Singh R. Why India could do with one more time zone. Univ Toronto. 2018;53(35):1–8.
46. Baheti R, Gill H. Cyber-hysical Systems. Impact Control Technol. 2011;12:161–6.
47. Reddy YB. Cloud-based cyber physical systems: design challenges and security needs. In: 10th International Conference on Mobile Ad-hoc and Sensor Networks; 2014, pp. 315–22.
48. Schneider D, Armengaud E, Schoitsch E. Towards trust assurance and certification in cyber-physical systems. Berlin: Springer; 2014.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.